This record is a partial extract of the original cable. The full text of the original cable is not available.

UNCLAS SECTION 01 OF 03 THE HAGUE 000799

SIPDIS

STATE FOR AC/CB, NP/CBM, VC/CCB, VC/VO, L/ACV, IO/S
SECDEF FOR OSD/ISP
JOINT STAFF FOR DD PMA-A FOR WTC
COMMERCE FOR BIS (GOLDMAN)
NSC FOR CHUPA
WINPAC FOR LIEPMAN

E.O. 12958: N/A
TAGS: PARM PREL CWC
SUBJECT: CHEMICAL WEAPONS CONVENTION (CWC): VIS ENHANCEMENT PROJECT, IMPLEMENTATION OF ISO 17799, SECURITY AUDITS, AND OTHER IT ISSUES AT THE TECHNICAL SECRETARIAT

This is CWC-43-04.

Status of VIS

¶1. (U) Del reps met with OPCW Chief of Administration Herb Schulz, Chief of the Information Support Branch (ISB) Greg Linden, and Chief of the Office of Confidentiality and Security (OCS) Rob Simpson to discuss issues related to Technical Secretariat (TS) work on the Verification Information System (VIS) Enhancement project on a number of occasions between March 2-26. Del reps stressed Washington's dissatisfaction with the speed of the TS implementation of the VIS effort. Linden and Simpson reported that the Deputy Director General heads the VIS project review board, and assesses VIS project status every two weeks.

¶2. (U) In summary, efforts to ensure the security of the Secure Critical Network (SCN) in parallel with development of the VIS project will cause a two-month delay in VIS deployment. But TS officials noted that if delegations need assurance that the SCN will appropriately protect their classified industrial data before submitting electronic data declarations, it is well worth the two-month investment.

VIS Enhancement Project

¶3. (U) Personnel from ISB, OCS, and the Verification Division are working closely on the VIS project. The prototype will be developed on an unclassified platform after documentation of the technical details, security assurances, and information flows are completed circa March 31. This definition and design phase is the critical underpinning of the effort and requires about 25 documents essential to understanding the project from the ISO and programming perspectives. The key VIS elements will be programmed over April/May, the remainder over the summer. Industrial data declarations are due April 1; the Verification Division and the Secure Critical Network (SCN) will be devoted to first entering and then assessing declared information received from around 50 States Party (SP) until late May.

¶4. (U) With the assistance of the Verification Division staff, ISB will assemble declaration data to test the VIS prototype capability in the June/July timeframe. Linden expects to be able to demonstrate the VIS prototype to users, both TS and SPs, by the end of the summer, even allowing for the annual and home leave plans of ISB staff and contractors. (Note: On January 1, 2004, ISB was approved a P2 position and has hired a programmer for the VIS project who will begin work in June. To supplement its VIS effort, ISB used a temporary hire to fill in.) In case of problems, Linden has programmed a two-month slip time (August to October). The enhanced VIS is expected to be fully up and running on March 31, 2005, for both the TS (80 percent of the users) and SPs (20 percent of users).

¶5. (U) Linden reported that a small number of SPs have approached him and asked to be allowed to submit their (redacted) industry declarations electronically in October ¶2004. Linden reported that the TS is considering how best to support this. One possibility under consideration (and will probably be approved) is mounting the Common File Transmission System (CFTS) interface and the chemical identifier database on the OPCW website. SPs who choose to do so can use the CFTS interface to format their data for submission to the TS.

Implementation of the ISO Standard 17799

¶6. (U) Simpson, who oversees the work of the Security Audit Teams (SAT), reported that the charter and mandate of SAT-IV

directs the auditors to assess security functionality. SAT-III recommended that the TS implement ISO standard 17799, which addresses the security management of system operations, which OCS is now working to implement. OCS has decided in principle to implement ISO 17799, but has yet to determine the cost of doing so. This will be reported to delegations in an upcoming DG note, which will include a recommendation to the EC that this standard be adopted.

¶7. (U) Simpson reported that at this point, the costs of implementing ISO 17799 will be minimal, mostly the result of training new staff members. Simpson also reported that this effort has been reported to the EC on a number of occasions. He also was surprised to find that a decision document regarding the ISO 17799 implementation had never gone to EC-29 as planned. This will be rectified, hopefully by EC-37 as one of the first elements emerging from the upcoming consultations on Confidentiality chaired by Del Rep.

¶8. (U) According to Linden, OCS decided on July 7, 2003 to accept the ISO 15408 standard or the "common criterion" which addresses security operations in a classified environment. There are five levels (EAL 1 to 5), and OCS wants to achieve EAL 3 from its starting point of zero (Note: EAL 3 is the standard set for secure U.S. Government systems). Linden noted that earlier SATs were not asked their opinion of the common criterion, nor has senior TS management been brought into the decision. (Note: This is a policy issue which needs senior level attention because of its cost and requirements to realign certain business procession, in particular the need to implement stringent documentation requirements.)

¶9. (U) Linden reported that the TS is not attempting to be accredited for either ISO standard. For the common criterion, there is no one authority that can certify EAL 3 implementation. Furthermore, it is very costly and would result in major delays in implementation of projects (Note: Certification for the common criteria would result in a delay of the RDBMS development effort for up to two years and cost at least USD 500,000).

¶10. (U) The documentation effort required by the two ISO standards has slowed things down, but no initiatives are dead in the water. In part, the effort is a result of the TS move from an organization that was not process-oriented to one that has appropriate managerial oversight and process procedures in place. Both OCS and ISB agree that in general more and better documentation is needed, and both share the ISO documentation burden. On the plus side, the TS has not had a systematic approach to documenting its IT efforts before. On the minus side, there is still no guidance from OCS regarding how much documentation is enough. Could the documentation effort be less onerous? Yes, the decision to go for EAL 3 for security assurance could be reversed. However, without documentation, the TS could not reassure the security auditors and SPs that things are as they should be. (Note: the RDBMS contractor analysis of its ability to meet the new (and last minute) security standard cost the project one month.)

Status of SCN Upgrade

¶11. (U) The upgrade of the SCN has been delayed until after EC-36. Taken together, a number of elements created challenges to this effort but will not seriously delay the SCN migration. Linden reported that the SCN upgrade will be completed and fully documented by July 1, 2004.

-- First, the seven new servers due in early December 2003 did not arrive until mid-February 2004.
-- Second, data migration from the 24 Microsoft Access databases is not technically difficult, and will require two days. This is complicated by a technicality: someone knowledgeable needs to map the new capabilities to the old ones, making the upgrades effort more difficult. The databases contain all the digitized declaration information that eventually will be sent to the RDBMS, so extra caution is needed to ensure that it is done right the first time.
-- Third, the inspector laptops are older models, and the upgrade to a powerful new operating system could tax their computing capability (tests show this will not be a problem). The laptops will be updated as they come in, circa ten or 12 a week. More difficult will be updates of the laptops at the CWDFs as they only return every six to eight months and carry unique software elements, so these laptops cannot simply be erased and reloaded.
-- Fourth, OCS requires more documentation to meet the ISO requirements, and ISB is preparing 30 documents. Because OCS needs time to review them, this led to a decision to delay until April/May.
-- Finally, Verification Division receives declarations in early April and produces the Verification Information Report in June, so it requested an additional delay until July. Upon reconsideration, Verification Division allowed that the upgrade probably could take place in early May, or perhaps

even in late April.

RDBMS and Security Audits

¶12. (U) Linden reported that the RDBMS specifics will also be fully documented by late June. Although ISB does not set the agenda for or time of audits, Linden suggested that the relevant RDBMS documentation could be put on a CD-ROM and distributed to SAT-IV for a remote July audit exercise. If SAT-IV sees itself as critical to the eventual acceptance of the Enhanced VIS project, the TS needs to know what SAT-IV perceives as its role and how it would exercise that role.

¶13. (U) In Linden's opinion, waiting to audit the RDBMS in December 2004 would be a mistake because the coding would have been completed by that time. Linden preferred to have SAT-IV assess the RDBMS documentation in July and to comment on any security concerns. (Note: Simpson/OCS also supports the idea of a remote Security Audit of the RDBMS design in the July timeframe.) Linden reported that the TS requested SAT-IV to provide by March 31 a list of tools (i.e., evaluation requirements and processes) they would like to use to assess the security functionality of the RDBMS development plans.

¶14. (U) Javits sends.
SOBEL